Derangements and Kronecker classes

Pablo Spiga

University of Milano-Bicocca
Dipartimento di Matematica e applicazioni
pablo.spiga@unimib.it

Napoli, AGTA Workshop-Reinhold Baer Prize 2024

A *fixed-point-free* element is a permutation with no fixed points (sometimes called *derangement*).
So, $(1, 2, 6, 10, 4)(3, 5)(7, 9, 8)$ is a fpf-element in $\mathrm{Sym}(10)$.

Theorem (Jordan)

Every transitive permutation group of degree > 1 *contains a fixed-point-free element.*

The proof is an application of the Orbit-counting lemma: the average number of fixed points is 1, but the identity fixes more than one element.

$$\frac{1}{|G|}\sum_{g\in G} |\operatorname{fix}(g)| = 1.$$

(for representation theorists: by the Frobenius reciprocity, the multiplicity of the trivial character in the permutation character is one)

The Erdős-Ko-Rado theorem

Let $\Omega = \{x_1, \dots, x_n\}$ be a finite set of size n and $\mathcal{F}$ a family of k-subsets of X, for $2k < n$. Suppose further that any two elements of $\mathcal{F}$ intersect in at least one element. Then

(*i*) $|\mathcal{F}| \leq \binom{n-1}{k-1}$;

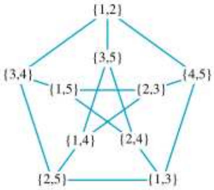
(*ii*) if $|\mathcal{F}| = \binom{n-1}{k-1}$, then all the k-sets in $\mathcal{F}$ contain a point $\overline{x}$ of X.

This result had great impact in combinatorics. There are many generalizations and analogues: partitions, uniform partitions, finite dimensional vector spaces, etc.

Some applications: rephrasing

The Kneser graph $K(n,k)$ is the graph whose vertices are the k-subsets of a set of size n and two vertices A, B are joined if $A \cap B = \emptyset$. The Petersen graph is an example of a Kneser graph, namely $K(5,2)$.

The Erdős-Ko-Rado theorem yields that an independent set of maximal size in $K(n,k)$, for $2k < n$, has size $\binom{n-1}{k-1}$. Also, the independent sets of maximal size are fully understood.



Erdős-Ko-Rado theorem for permutation groups

Given two permutations g, h in $\mathrm{Sym}(n)$, we say that g, h are intersecting if $\mathrm{fix}(g^{-1}h) \neq \emptyset$.

What is the maximal size of an intersecting set of permutations in $\mathrm{Sym}(n)$?

Maybe...$(n-1)!$...

What are the sets attaining this bound?

Maybe...the cosets of the stabilizer of a point...

Graph-theoretic terminology

Let D be the set of derangements of $\mathrm{Sym}(n)$ (i.e. fixed-point-free elements). The derangement graph $\Gamma_{\mathrm{Sym}(n)}$ of $\mathrm{Sym}(n)$ is the graph whose vertices are the elements of $\mathrm{Sym}(n)$ and whose edges are the pairs $\{g, h\}$ such that $g^{-1}h$ is a derangement.

Note that the right regular representation of $\mathrm{Sym}(n)$ is a subgroup of $\mathrm{Aut}(\Gamma_{\mathrm{Sym}(n)})$. So, $\Gamma_{\mathrm{Sym}(n)}$ is a Cayley graph, i.e. $\Gamma = \mathrm{Cay}(\mathrm{Sym}(n), D)$.

An independent set for Γ is simply an intersecting set for $\mathrm{Sym}(n)$.

Lemma

Let Γ be vertex-transitive graph, C a clique of Γ and S an independent set of Γ. Then $|C||S| \leq |\Gamma|$. Equality is met if and only if $|C^g \cap S| = 1$, for every $g \in \mathrm{Aut}(\Gamma)$.

In the derangement graph $\Gamma_{\mathrm{Sym}(n)}$, any regular subgroup C of $\mathrm{Sym}(n)$ is a clique of size n. Thence, if S is an independent set, we get

$$|S| \leq \frac{n!}{n} = (n-1)!.$$

Hard to understand whether the independent sets of maximal size are cosets of the stabilizer of a point.

Cameron-Ku and Larose-Malvenuto proved that every independent set of maximal size of $\Gamma_{\mathrm{Sym}(n)}$ is the coset of the stabilizer of a point.

More recently, Godsil-Meagher proved the same result using the character theory of $\mathrm{Sym}(n)$.

Erdős-Ko-Rado type of theorems have been proved for many classes of permutation groups. This is a typical example.

Theorem

Any independent set of maximal size of the derangement graph of $\mathrm{PGL}(n+1, q)$ acting on the projective space $\mathbb{P}_q^n$ is either the stabilizer of a point or the stabilizer of a hyperplane.

Incidentally, using Gauss sums one can prove stability results for large independent sets.

Density

In general only rarely G_ω is an intersecting set of maximal size in G and hence no analogue of the Erdős-Ko-Rado theorem holds for arbitrary permutation groups. For instance, if we let the alternating group $\mathrm{Alt}(5)$ acting on the ten 2-subsets of $\{1, 2, 3, 4, 5\}$, we see that $\mathrm{Alt}(4)$ is an intersecting set of size 12, whereas the point stabilizer in this action has only cardinality 6.

Even when $|G_\omega|$ is the maximal cardinality of an intersecting set for G, it is far from being true that all intersecting sets attaining the bound $|G_\omega|$ are cosets of the stabilizer of a point.

Let $\omega \in \Omega$ with G_ω having maximum cardinality among point stabilizers. The intersection density of the intersecting family $\mathcal{F}$ of G is defined by

$$\rho(\mathcal{F}) = \frac{|\mathcal{F}|}{|G_\omega|}$$

The intersection density of G is

$$\rho(G) = \max\{\rho(\mathcal{F}) \mid \mathcal{F} \subseteq G, \mathcal{F} \text{ is intersecting}\}.$$

This invariant was introduced by Li, Song and Pantagi in to measure how "close" G is from satisfying the Erdős-Ko-Rado theorem.

Jordan's theorem revised

The clique-coclique bound

$$\alpha(\Gamma_G)\omega(\Gamma_G) \leq |V\Gamma_G| = |G|$$

can be used to extract useful information on the intersection density of G. Indeed, from the definition of intersection density, we obtain

$$\rho(G) \leq \frac{|\Omega|}{\omega(\Gamma_G)}.$$

When G is transitive and $|\Omega| \geq 2$, Jordan's theorem ensures that G has a derangement g and hence $\{1, g\}$ is a clique of Γ_G of cardinality 2. Therefore, we have

$$\rho(G) \leq \frac{|\Omega|}{2}.$$

Meagher, Razafimahatratra and Spiga have shown that, when G is transitive and $|\Omega| \geq 3$, the derangement graph Γ_G has a clique of cardinality 3, that is a triangle. Hence $\omega(\Gamma_G) \geq 3$ and

$$\rho(G) \leq \frac{|\Omega|}{3}.$$

Despite the fact that Jordan's theorem is elementary, the proof of this theorem is quite involved and ultimately relies on the Classification of the Finite Simple Groups. A key ingredient is a theorem of Saxl.

Theorem

Let T be a non-abelian simple group, let G be an almost simple group having socle T and let H be a subgroup of T. If

$$T = \bigcup_{g \in G} H^g,$$

then $H = T$.

In the light of these two results, Meagher, Razafimahatratra and Spiga ask for the existence of a function $f : \mathbb{N} \to \mathbb{N}$ such that, if G is transitive of degree n and Γ_G has no k-clique, then $n \leq f(k)$.

Indeed, when $k = 2$, we have $n \leq 1$ by Jordan's theorem and, when $k = 3$, we have $n \leq 2$ by the existence of triangles in derangement graphs of transitive groups of degree at least 3.

This is a first step towards a positive answer to the question above.

Theorem (Fusari, Previtali, Spiga)

There exists a function $f_1 : \mathbb{N} \to \mathbb{N}$ such that, if G is innately transitive of degree n and the derangement graph of G has no clique of size k, then $n \leq f_1(k)$.

In particular, we have an affirmative answer for innately transitive groups. By keeping track of the function f_1, we have this refined statement when $k = 3$.

Theorem

If G is innately transitive of degree n and the derangement graph of G has no clique of size 4, then $n \leq 3$.

Theorem (Gogniat, Spiga)

If G is transitive of degree n and the derangement graph of G has no clique of size 4, then $n \leq 30$.

There are some remarkable connections between normal coverings and algebraic number fields.
Given an algebraic number field k and a finite extension field K of k the Kronecker set of K over k is the set of all prime ideals of the ring of integers of k having a prime divisor of relative degree one in K. Then, two finite extensions of k are said to be Kronecker equivalent if their Kronecker sets have finite symmetric difference, that is, the Kronecker sets differ only in at most a finite number of primes. This defines an equivalence relation and such extensions are said to belong to the same Kronecker class.

Let K and K' be finite extensions of a given fixed algebraic number field k and let M be a Galois extension of k containing K and K'. Let $G = \mathrm{Gal}(M/k)$, $U = \mathrm{Gal}(M/K)$ and $U' = \mathrm{Gal}(M/K')$. It is shown by Jehne that K and K' are Kronecker equivalent if and only if

$$\bigcup_{g\in G} U^g = \bigcup_{g\in G} U'^g.$$

Conjecture (Neumann, Praeger)

There is an integer function f such that, if G is a finite group with subgroups U, U' such that $|G : U'| = n$ and

$$\bigcup_{g \in G} U^g = \bigcup_{g \in G} U'^g,$$

then $|G : U| \leq f(n)$.

This conjecture phrased in terms of Kronecker classes is as follows.

Conjecture

There is an integer function f such that, if K/k is an extension of degree n of algebraic number fields and L/k is Kronecker equivalent to K/k, then $|L : k| \leq f(n)$.

The Neumann-Praeger Conjecture can be phrased in terms of permutations groups. Let G, U, U' be as in the statement of the conjecture and let Ω be the set of right cosets of U in G. Now,

$$\bigcup_{g\in G} U^g$$

is the set of elements of G fixing some element of Ω. If this union equals $\bigcup_{g\in G} U'^g$ and $|G : U'| = n$, then a clique in the derangement graph of G in its action on Ω has cardinality at most n. In fact, let C be a clique of size greater than n. Then by the pigeonhole principle, C intersects a coset of U' in at least two elements. Then the ratio xy^{-1} lies in U' and hence xy^{-1} is conjugate to an element of U. Therefore, xy^{-1} fixes some point, contradicting the fact that C is a clique. Therefore the Neumann-Praeger Conjecture can be seen as a particular case of the question of Meagher, Razafimahatratra and Spiga on cliques in derangement graphs.

Theorem (Fusari, Harper, Spiga)

There exists a function $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *such that the following holds. Let* G *be a finite group, let* $U \leq G$ *and let* $\mathrm{Inn}(G) \leq A \leq Aut(G)$ *with* $|A : \mathrm{Inn}(G)| = n$*. Write* c *for the number of* A*-chief factors of* G/U_A*. If* $G = \bigcup_{a \in A} U^a$*, then* $|G : U| \leq g(n, c)$*.*

In particular, this gives a partial answer to the conjecture of Neumann and Praeger, if we allow to also use the number of chief factors of the group.

Jordan's observations can be phrased entirely in a group-theoretical terminology. The elements of G fixing some point of Ω are the elements contained in some point stabilizer G_ω and hence the elements in

$$\bigcup_{\omega \in \Omega} G_\omega = \bigcup_{g \in G} G_{\omega_0}^g.$$

Therefore Jordan's theorem says that $\bigcup_{g \in G} G_{\omega_0}^g$ is a proper subset of G. In other words,

A finite group cannot be the union of the conjugates of a proper subgroup.

Infinite groups can be the union of the conjugates of a proper subgroup: the HNN-extension allows to construct easily a group where any two non-identity elements are conjugate.

In the realm of finite groups, we might be interested in investigating finite groups G admitting two proper subgroups H and K with

$$G = \bigcup_{g \in G} H^g \cup \bigcup_{g \in G} K^g.$$

For instance, $G := \mathrm{Sym}(3)$ is the union of the conjugates of $\mathrm{Alt}(3)$ and $\langle (1,2) \rangle$.

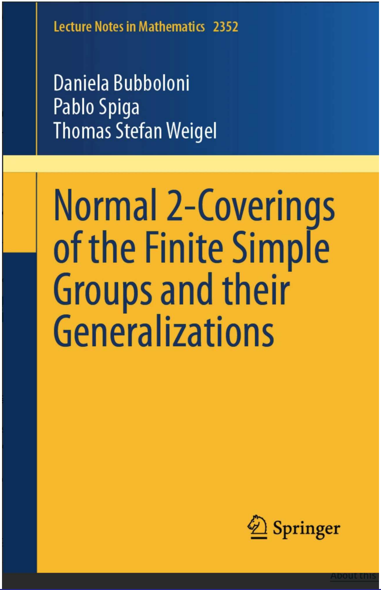
Definition

Let k be a positive integer and let G be a finite non-cyclic group. A ***normal k-covering*** of G is a set $\mu = \{H_1, \dots, H_k\}$ of k proper subgroups of G with the property that every element of G belongs to the conjugate H_i^g, for some $i \in \{1, \dots, k\}$ and for some $g \in G$, that is,

$$G = \bigcup_{i=1}^{k} \bigcup_{g \in G} H_i^g.$$

We refer to $H_1, \dots, H_k$ as the ***components*** of μ. If $H_1, \dots, H_k$ are maximal subgroups of G, we refer to them as ***maximal components***. The ***normal covering number*** of the group G, denoted by $\gamma(G)$, is the smallest integer k such that G admits a normal k-covering. Note that in a normal k-covering $\{H_1, \dots, H_k\}$ with $k = \gamma(G)$, the proper subgroups $H_1, \dots, H_k$ are in distinct G-conjugacy classes.

Garonzi and Lucchini (and independently Cheryl Praeger) have a paper concerning coverings and normal coverings of finite groups where they give a broad recipe for determining the normal covering number of a finite group, using its composition factors. This recipe is most efficient for finite groups having covering number 2. In the light of this reduction, but also for intrinsic interest, we aim (Daniela Bubboloni, myself and Thomas Weigel) to give a classification of the *almost simple groups having normal covering number 2*.


Lecture Notes in Mathematics 2352
Daniela Bubboloni
Pablo Spiga
Thomas Stefan Weigel
Normal 2-Coverings of the Finite Simple Groups and their Generalizations
Springer